PREDICTIVE POLICING

Department Setup Guide

Revised: February 4, 2013

Overview

Getting started involves three easy steps:

1) We will send you a Spreadsheet, requesting information about how your department operates and how crimes are classified.

2) Separately, we will work with your Technical Staff to install our software on one of your servers.

3) Finally, we will setup accounts for your command staff and officers, granting access to the application.

Contact with the department's Technical Staff needs to happen as early as possible to ensure a smooth and quick set-up process. It is also important that they receive a copy of this Department Setup Guide, as it will answer many (if not all) of their questions.

Information Gathering

We need the following information to get started:

- Shift Schedules, including the name for each Shift.

- Desired Crime Types, such as "Robbery" and "Auto Theft"

- Crime Codes for the above Crime Types.

- Prediction addresses to exclude, such as Police Stations.

This information is collected on the provided Customer Setup Form.

We need to know who should have access to the PredPol application itself. We need the following information to give them access:

- First and last name.

- E-Mail Address.

- Role: Officer? Command Staff?

Finally, we need some basic technical information that might require you to ask your Technical Staff:

- What type of RMS is currently in use?

- What is the underlying database engine supporting the RMS? e.g., mySQL, Oracle, Microsoft SQL, custom

- What Operating System and Browser will the server be using?

- On which database tables does the crime data reside?

Technical Setup

For our software to work successfully, we need to ensure that the following takes place:

- Software installed on a Server that runs 24/7.
- At minimum, server has: 10GB free disk-space and 2GB RAM.
- Network access to the Crimes Database.
- Credentials with read-access to the Crimes Database.
- Outbound access to PredPol Servers (Internet).

PredPol takes security very seriously; we collect the least amount data necessary to make our predictions. Strong Encryption is used to secure the crime data, before transmitting it over a verified HTTP/SSL connection. Our servers are secured, monitored, and undergo a routine security review—including periodic Penetration Testing. All Department data is stored in isolation, and we make sure to only obtain the least data necessary to meet our contractual obligations.

Please reach out to your PredPol Contact if there are custom needs for your Department.